Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of *Advanced Methods to Target and Eliminate Unlawful Robocalls*	CG Docket No. 17-59

COMMENTS OF NEUSTAR, INC.

July 3, 2017

Leonard J. Kennedy
Aaron N. Goldberger
Richard L. Fruchterman, III
NEUSTAR, INC.
1775 Pennsylvania Avenue N.W.
4th Floor
Washington, D.C. 20006

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of *Advanced Methods to Target and Eliminate Unlawful Robocalls*	CG Docket No. 17-59

COMMENTS OF NEUSTAR, INC.

I. INTRODUCTION AND SUMMARY

Neustar, Inc. ("Neustar") hereby submits the following comments in response to the Federal Communication Commission's ("FCC" or "Commission") *Robocalling Notice* regarding methods to identify and eliminate unlawful robocalling.[1] Neustar fully supports the Commission's efforts to protect consumers from unlawful robocalls, which are not only annoying but also harmful to consumers.[2] As the neutral third-party administrator of U.S. numbering databases and an industry leader in the development of solutions to mitigate unwanted robocalls and Caller ID spoofing, Neustar stands ready to assist the Commission's efforts.

Neustar supports the Commission's proposed rules to allow service providers to block calls that appear to be originated from telephone numbers that the subscriber has asked not to be

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Notice of Proposed Rulemaking and Notice of Inquiry, FCC 17-24 (*"Robocalling Notice*").

[2] *Robocalling Notice* ¶ 2; *see also Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, File No.: EB-TCD-15-00020488, Notice of Apparent Liability for Forfeiture, FCC 17-80 (rel. June 22, 2017) (proposing a penalty of $120 million against individual and his associated companies for making more than 96 million illegally spoofed robocalls with the intent to cause harm).

permitted to originate calls or from telephone numbers that are invalid or unallocated, whether those calls are initiated domestically or internationally. As the North American Numbering Plan Administrator ("NANPA") and Thousands-block Pooling Administrator ("PA"), Neustar can facilitate service providers' ability to block such calls that are determined to be illegal robocalls or Caller ID spoofed calls using objective standards applicable across all network technologies. Even with objective standards, though, care must be taken to ensure legitimate calls are not caught in the blocking net.

Efforts to identify and block illegal robocalls or Caller ID spoofed calls that rely on less objective standards, however, can lead to undesired results. Although the goal of blocking these calls is worthy, it is a highly complicated process fraught with real risks of blocking legitimate traffic. Not only could blocking of legitimate traffic be difficult to reverse, it could also damage businesses and other organizations that rely on legitimate robocalling to remain in contact with customers or spoof the Caller ID legally to protect the identity or location of the caller. Neustar's comments focus on helping the FCC distinguish between blocking techniques and policies that are truly helpful and those that could prove to be harmful or costly to implement or manage. Neustar also recommends that the Commission encourage approaches that put more information regarding the identity of a caller into the hands of consumers. Armed with such information, consumers can make more informed decisions whether a call should be answered, ignored, or blocked. This approach balances industry action and consumer choice – a balance that Neustar believes is the most effective solution to eliminating unlawful robocalling and Caller ID spoofing.

II. BACKGROUND

Neustar is a neutral third-party provider of a variety of telecommunications-related products and services throughout the United States. Neustar currently serves as the NANPA and

PA under separate federal contracts with the FCC.[3] Neustar also serves as the Local Number Portability Administrator ("LNPA"), which manages the regional Number Portability Administration Centers ("NPACs").[4] As the current NANPA, PA, and LNPA, Neustar is in a unique position to comment on how these systems can contribute to the Commission's goal of targeting and eliminating illegal robocalling and Caller ID spoofing.

Neustar is also the largest U.S. provider of caller name ("CNAM") services that authenticate and display names with the calling telephone number. In coordination with its service provider customers, Neustar has been actively developing solutions to identify suspect calls and to provide end users significantly more information about the calling party to mitigate illegal or unwanted robocalls and Caller ID spoofing.

Consumers are inundated with unwanted and illegal robocalls, which continue to be the Commission's number one source of consumer complaints.[5] Consumers get annoyed at the time they waste answering unwanted calls and lose hundreds of millions of dollars every year to fraud enabled by illegal robocalling and Caller ID spoofing. To address this problem, the Internet Engineering Task Force ("IETF") Secure Telephone Identity Revisited ("STIR") working group drafted three related standards that collectively define a means to authenticate the calling party

[3] Neustar has served as the NANPA since 1997 pursuant to orders of the FCC. Neustar has served as the PA since the first contract was awarded via competitive bidding process in 2001 – a contract that was renewed via competitive bidding in 2007.

[4] Neustar has served as the LNPA in each of the seven NPAC regions since 1997.

[5] *See, e.g.,* Robocall Strike Force Report, at 1 (Oct. 26, 2016) ("What was once a nuisance has become a plague to U.S consumers receiving an estimated 2.4 billion robocalls per month in 2016"), *available at* https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf; *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Declaratory Ruling and Order, 30 FCC Rcd 7961, ¶ 1 (2015).

number, securely transport this information "on the wire" and verify it at the receiving end.[6] Neustar co-authored these three IETF standards.

To put these standards into action, the Alliance for Telecommunications Industry Standards ("ATIS") has developed Signature-based Handling of Asserted information using toKENs ("SHAKEN"), a trusted identity framework that provides guidance for service providers implementing Caller ID network validation. Neustar has been a contributor to the two joint ATIS/SIP Forum SHAKEN framework documents.[7]

Together, the IETF STIR standards and the ATIS SHAKEN framework give service providers the tools they need to authenticate, digitally sign, and verify calling party numbers. This functionality enables service providers to identify suspicious calls before they reach their customers, and provide notifications that allow consumers to decide whether to answer a call. SHAKEN also includes important capabilities to assist law enforcement in finding the source of unwanted calls.

On February 2, 2017, ATIS announced that it had launched the ATIS Robocalling Testbed, a virtualized testbed to advance the SHAKEN framework, and appointed Neustar as the exclusive provider of the standing testbed.[8] The ATIS Robocalling Testbed facilitates interoperability testing, which helps service providers, suppliers, and third parties test SHAKEN by generating end-to-end calls that include all network functions. The testbed provides

[6] *See* Authenticated Identity Management in the Session Initiation Protocol (SIP) (https://datatracker.ietf.org/doc/draft-ietf-stir-rfc4474bis/); Personal Assertion Token (PASSporT) (https://datatracker.ietf.org/doc/draft-ietf-stir-passport/); Secure Telephone Identity Credentials: Certificates (https://datatracker.ietf.org/doc/draft-ietf-stir-certificates/).

[7] *See* ATIS-1000074, Signature-based Handling of Asserted information using toKENs (SHAKEN) (http://www.atis.org/); ATIS-1000080 (pending approval), SHAKEN: Governance Model and Certificate Management (http://www.atis.org/).

[8] Press Release, *ATIS Launches Industry Testbed to Advance Mitigation of Unwanted Robocalling and Called ID Fraud* (Feb. 2, 2017), *available at* https://sites.atis.org/insights/atis-launches-industry-testbed-advance-mitigation-unwanted-robocalling-caller-id-fraud/.

configurations to test individual SHAKEN components or complete network implementations and is open to all service providers with an operating carrier number.[9]

III. DISCUSSION

A. Blocking at the Request of Subscribers for Their Assigned Numbers is Reasonable, but Presents Challenges to Implement.

Although provider-initiated (or network) blocking is an important tool to combatting robocalling, this tool should be permitted only in circumstances when it can be objectively determined that a call is an illegal robocall or has been illegally spoofed. Empowering subscribers is a critical piece of the mitigation puzzle in the fight against illegitimate robocalling and spoofing. Neustar supports allowing a subscriber, who only wants to receive calls, to request blocking of outbound calls from their assigned telephone number to prevent spoofing (*e.g.*, a government agency such as the Internal Revenue Service ("IRS")).[10] In this case, the subscriber is consenting to have calls that originate from its telephone number blocked to eliminate the risk of potential fraud. It can be objectively determined that the subscriber's number is on a "Do-Not-Originate" ("DNO") list; therefore the subscriber's provider blocks calls that appear to originate from that number and, as discussed below, requests other providers to do the same.[11]

Because this approach is initiated by – and necessarily requires the consent of – the subscriber, the risk that a service provider will inadvertently block legitimate traffic appears

[9] *See* Robocall Strike Force Report, at 6 (April 28, 2017), *available at* http://www.atis.org/01_strat_init/Robocalling/docs/Ex%20Parte-Strike-Force-Report-2017-04-28-FINAL.PDF.

[10] *Robocalling Notice* ¶ 14; *see also* Public Notice, *Consumer and Governmental Affairs Bureau Clarification on Blocking Unwanted Robocalls*, 31 FCC Rcd 10961 (CGB 2016) ("*2016 Guidance PN*").

[11] In addition to calls that appear to be from DNO telephone numbers, Neustar believes that calls that appear to be from invalid or unallocated numbers are also objectively illegal because none of these numbers should be originating calls. *Robocalling Notice* ¶¶ 17, ¶ 19. As a result, service providers should not be required to obtain consent from the called party to block calls from DNO, invalid, or unallocated numbers. *Robocalling Notice* ¶ 25.

small. However, that does not mean there is no risk at all. Providers will need to ensure subscriber consent is legitimate and outbound calling for a number is not blocked at the request of a party without authorization to make that request. There may be other operational challenges with implementing and managing this blocking option that service providers will need to address.

Although it may be advantageous to maintain a database of consented-to DNO numbers (*e.g.*, numbers associated with the IRS),[12] some service providers may not be able to implement this blocking solution within their network. In those instances, a modified DNO solution can still work by informing the subscriber through the Caller Name display that the call is "Fraudulent." Any consented-to DNO numbers can be loaded in recognized industry CNAM databases to provide the "Fraudulent" display to protect consumers when their provider is not able to support DNO call blocking.[13]

Further, a subscriber's request to its service provider to block calls from a particular telephone number will only be effective if other providers know not to terminate calls from that telephone number. Thus, providers must have a means of communicating in real time both blocking and unblocking requests from other providers, as well as establishing reasonable timeframes for all providers to act on these requests. Establishing a system to maintain this information could be costly, and it is not clear that such a system could be implemented without the risk that legitimate calls will be blocked in error. While Neustar supports blocking of calls at the request of the originating subscriber, a close examination of the costs and risks involved may

[12] *2016 Guidance PN* at 2.

[13] It should be noted that determining the calling name is the responsibility of the called party's terminating carrier. For each call, the terminating carrier will do a look-up, or dip, into a CNAM database to determine the name that is currently registered to the caller's telephone number.

lead to the conclusion that it is more beneficial in the long run for the Commission to consider ways to advance the deployment of caller authentication standards like STIR/SHAKEN to address the root problem of unlawful robocalling and Caller ID spoofing.

B. Service Providers Should be Permitted to Block Calls Originating from Invalid Numbers.

As noted above, network call blocking is a necessary tool to reduce unlawful robocalling, such as DNO calls. Another circumstance in which this tool should be employed is when a call originates from an invalid number. Neustar supports the Commission's proposal to allow provider-initiated blocking of calls originating from numbers that are not valid.

Examples of invalid telephone numbers include those where the Numbering Plan Area (NPA or area code) begins with the 0 or 1 digit or the NXX (central office code or CO code) begins with the 0 or 1 digit. In both these cases, no valid calls could originate from such numbers. Additionally, there are other telephone number combinations from which calls should not originate, such as certain NXXs where restrictions have been placed in specific state jurisdictions or NPAs on inward dialing only, which vary by jurisdiction (NPA or state). Other examples of invalid numbers are N11 (911, 211, etc.), 976, and 555 NXXs.

As the NANPA and PA, Neustar maintains information for invalid numbers within the North American Numbering Plan ("NANP"), and the industry has other sources to identify invalid numbers such as ATIS's Industry Numbering Committee ("INC"). Thus, service providers already have access to the information they need if they choose to block calls that appear to originate from invalid numbers in response to a Commission rule permitting them to do so.

C. Service Providers Should be Permitted to Block Calls Originating from Valid But Unallocated Numbers, Although it Will be Necessary to Put a Process in Place to Implement This Rule.

Neustar supports the FCC's proposal to allow provider-initiated blocking of calls from numbers that are valid but have not yet been allocated by the NANPA or the PA.[14] These unallocated numbers should not be making calls and include telephone numbers in: (1) unallocated area codes in the NANP; (2) unallocated geographic Central Office ("CO") codes (NPA-NXX) in the United States; and (3) unallocated non-contaminated thousands-blocks (NPA-NXX-X) in the United States.[15]

It is the proper function of the numbering administrator to provide unallocated number information. While this information is currently available through various public reports on the NANPA and PA websites, it should be more comprehensive and updated daily. Specifically, a process should be established by which the NANPA and the PA will provide on their websites: (1) "Blacklists" of unallocated numbers that should not be making calls; and (2) "Whitelists" of allocated area codes in the NANP, allocated geographic CO codes in the United States, and allocated thousands-blocks in the United States. In its capacity as the NANPA and the PA, Neustar commits to working collaboratively with the Commission and the industry to develop a process that will meet service provider and subscriber needs in implementing any rule permitting the blocking of calls from valid but unallocated telephone numbers.

[14] *Robocalling Notice* ¶ 19.

[15] Because thousands-blocks that have been donated by code-holders may contain individual telephone numbers that have been assigned to subscribers, this "contamination" should exclude the block from being considered "unallocated." Furthermore, the NANPA does not administer codes outside the United States, specifically in Canada and Caribbean countries, or toll-free numbers. Thus, other arrangements would need to be made to identify unallocated numbers that the NANPA does not administer.

D. Allowing Service Providers to Block Calls Originating from Numbers Allocated to a Provider But Not Assigned to a Subscriber Would be Problematic to Implement.

Neustar does not oppose the Commission's proposed rule to allow provider-blocking of calls from numbers that have been allocated to a provider but not assigned to a subscriber at the time of the call. However, Neustar is unaware of any existing means to implement this well-intentioned proposal.[16] While Neustar as the NANPA collects information from providers on the quantity of numbers assigned to subscribers via Numbering Resources Utilization Forecasting ("NRUF") data, it does not collect information on the individual numbers that are unassigned. And, to Neustar's knowledge, no master list of assigned or unassigned numbers exists today.

While each individual service provider certainly knows which telephone numbers it has been allocated but not yet assigned to subscribers, Neustar has learned during its years as a numbering administrator that service providers often consider such information to be competitively sensitive. While it may be possible to involve a neutral third party to collect allocated but unassigned telephone number information from service providers and disseminate it among the industry, such involvement would take time and could be costly. Furthermore, because service providers assign telephone numbers nearly every minute of every day, any third-party system would have to be capable of being updated on a nearly instantaneous basis; otherwise, the risk exists that calls will be blocked in error after the blocked number that was unassigned, for example, in the morning is assigned to a subscriber in the afternoon.

The Commission seeks comment on whether the NPAC could be a source of information regarding unassigned telephone numbers.[17] The NPAC does not have this capability for two reasons. First, the NPAC, with few exceptions, only includes assigned numbers that have been

[16] *Robocalling Notice* ¶ 21.

[17] *Robocalling Notice* ¶ 22.

ported. Numbers assigned from a provider's native inventory are not required to be included in the NPAC. Second, although the NPAC supports a process to remove ported telephone numbers when subscribers disconnect service that allows the number to "snap-back" to the provider originally allocated the number, not all service providers adhere to this process in the same manner. Further, there is no notification to the NPAC when a number that has been snapped back is then reassigned to another subscriber.

In short, the Commission's proposal to permit service providers to block allocated but unassigned telephone numbers raises potential competitive concerns and presents serious implementation challenges. Given these uncertainties, the Commission should instead consider ways to promote the deployment of other mitigation techniques, such as STIR/SHAKEN, to address the problem of calls appearing to originate from unassigned numbers.

E. Providers Should Be Permitted to Block Internationally Originated Calls With U.S. Numbers Under The Same Circumstances When Blocking of Domestic Calls is Permissible.

A significant number of illegitimate calls originate from outside the United States. Many international calls appear as legitimate to providers because they use NANP telephone numbers that are spoofed at origination, or by some intermediate provider or international gateway provider. As discussed above, calls that appear to be from numbers that the subscriber has asked not to originate calls, from invalid numbers, or from unallocated numbers can be blocked by providers with little serious risk that legitimate calls will not be completed. Thus, Neustar sees no reason why the same blocking rules applicable to domestic originated calls should not also apply to internationally originated calls. [18]

[18] *Robocalling Notice* ¶ 24.

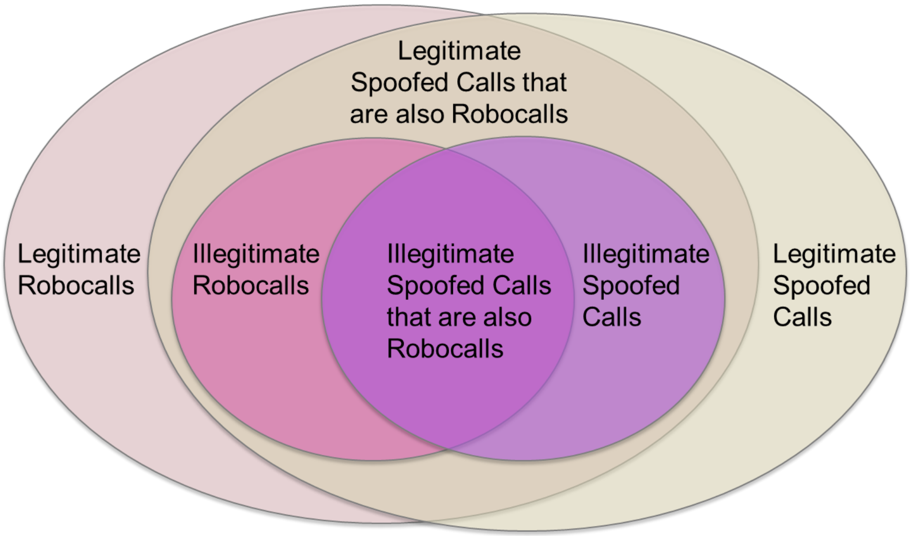
F. The FCC Must Consider the Need for Coordinated Provider Blocking and Unblocking of Calls from Individual Numbers.

If the Commission adopts rules that allow service providers to block terminating calls based on DNO requests from subscribers or to block calls that appear to be from unassigned numbers, it should consider the associated management process. Changes to blocking requests as well as changes to unassigned numbers will need to be tracked and then shared among providers. It may be most efficient to centralize this information-sharing function and incorporate into an established industry service, such as the NANPA or PA, or the industry Line Information Databases. As noted above, because NANPA and PA already have authoritative numbering data regarding invalid and unallocated numbers that could support provider blocking, it may be possible to augment these systems to manage and distribute information about DNO requests and unassigned numbers.

G. The FCC Should Only Permit Service Providers to Block Calls Based on Objective Standards for Identifying Illegal Calls.

As noted above, Neustar supports efforts to block calls from telephone numbers that can objectively be determined to be illegitimate robocalling or spoofing, such as subscriber requests for DNO and invalid or unallocated telephone numbers. Beyond calls from these types of telephone numbers, however, Neustar believes that giving service providers greater latitude to block calls to address potential unlawful robocalling or Caller ID spoofing makes the process more subjective and increases the risk that lawful calls will be blocked, even inadvertently.

To be sure, the process of segregating lawful and unlawful calls involving robocalling and Caller ID spoofing is complicated. This complexity is illustrated at a high level by the following figure:[19]


Legitimate Spoofed Calls that are also Robocalls
Legitimate Robocalls
Illegitimate Robocalls
Illegitimate Spoofed Calls that are also Robocalls
Illegitimate Spoofed Calls
Legitimate Spoofed Calls

Spoofing is a technique that deliberately falsifies the Caller ID information to disguise the identity of the calling party. However, there are legitimate use cases and conditions when Caller ID information is spoofed (*e.g.*, doctor's offices after hours call services and abused women's shelters), and only spoofing undertaken "with the intent to defraud, cause harm, or wrongfully obtain anything of value" is prohibited.[20]

Robocalling is a technique that uses a computerized auto-dialer to deliver a pre-recorded message, often associated with telemarketing campaigns. As with spoofing, there are legitimate

[19] Reproduced from ATIS-0300114, "Next Generation Interconnection Interoperability Forum (NGIIF) Next Generation Network (NGN) Reference Document Caller ID and Caller ID Spoofing."

[20] Truth in Caller ID Act, 47 U.S.C. § 227(e); *see also Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, 26 FCC Rcd 9114 (2011).

use cases and conditions when robocalling is permitted, and prohibited practices involving robocalling are spelled out in the TCPA and the FCC's implementing rules.[21]

In practice, identifying incidents of legitimate versus illegitimate Caller ID spoofing and robocalling is a difficult task. Other than the Caller ID information, service providers have no way of knowing in advance what the actual purpose or intent of any call is. Thus, the risk exists that a service provider will block legitimate calls, particularly given the inherent difficulty in determining the legitimacy of calls with absolute accuracy in the absence of objective standards as discussed in conjunction with subscriber requested DNO, or invalid or unallocated numbers.

Neustar believes that a broad range of mitigation approaches are or will be available to address unlawful robocalls and spoofing that do not require service providers to make highly subjective determinations about whether a particular call is illegal. These commercially available approaches include algorithmic solutions ranging from crowdsourcing to network-based volumetric and forensic data analysis. For example, T-Mobile launched Scam ID in March 2017, which is a network call data analysis and heuristics solution that identifies calls from known phone scammers, across all handset platforms, on smartphones and feature phones. If a scam call is detected, the Caller ID will display "Scam Likely" on the device, giving customers the option to answer, or permanently block the number. Customers that choose to invoke Scam Block, another free service offered by T-Mobile, will have all calls from known scammers blocked.[22]

While heuristic approaches are ill-suited to network-based call blocking, they can put meaningful information in the hands of consumers, allowing them to then make more informed

[21] Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227(a), (b); *see also* 47 C.F.R. § 64.1200(a)(3).

[22] *See* Robocall Strike Force Report, at 18 (April 28, 2017), *available at* http://www.atis.org/01_strat_init/Robocalling/docs/Ex%20Parte-Strike-Force-Report-2017-04-28-FINAL.PDF.

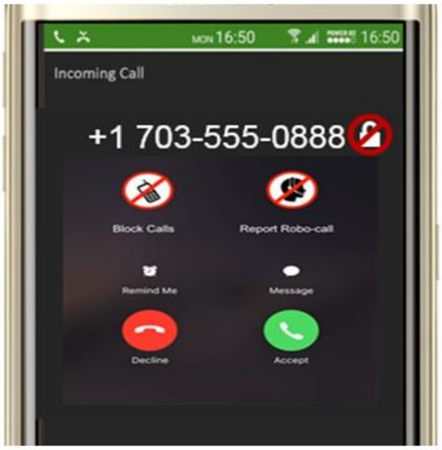
decisions as to whether to answer a call. In addition, the STIR and SHAKEN standards will enable service providers and consumers to identify illegitimate spoofing over VoIP-based network infrastructure, and to trace such activity back to the authenticating party. Neustar believes the FCC should encourage industry adoption of the entire range of these mitigation approaches, rather than allowing service providers to block calls based on highly subjective determinations.

Neustar also supports use of the currently available, and for all practical purposes, ubiquitous CNAM infrastructure in the United States to better inform subscribers of the types of calls they are receiving. For example, Verizon has detailed its trialing of a solution utilizing the CNAM infrastructure within the Industry Robocall Strike Force Report from April 28, 2017.[23] This type of solution is now readily available through recognized CNAM service providers and, importantly, is an option for service providers that still operate a traditional TDM telecommunications network.

This approach uses the development and integration of analytics, some rooted in actual call data, which can be effective at detecting illegal robocall activity. Supplemented with other data (*e.g.*, crowdsourcing from subscribers, known good actors), calls can be categorized and/or scored with useful information and then signaled to the subscriber over the currently available CNAM infrastructure. Conventional CNAM supports a 15 alphanumeric character field that is already signaled from any network and displayable on most landline (directly or through a connected caller name display unit) and mobile devices today. This approach can be

[23] *See* Robocall Strike Force Report, at 18 (April 28, 2017), *available at* http://www.atis.org/01_strat_init/Robocalling/docs/Ex%20Parte-Strike-Force-Report-2017-04-28-FINAL.PDF.

implemented on any provider network today since it is technology agnostic.[24] For smartphone operating systems/applications, this approach can leverage growing device processing capabilities and larger displays, providing the subscriber with more detailed information about the caller, beyond just a 15-character name and phone number. Providing consumers with more information about the calling party, including the verification status of the calling party, allows the consumer to have more control over what calls they answer and to have greater trust in Caller ID and CNAM.



Despite the benefits of approaches using data analytics in detecting certain types of illegal calls, Neustar believes that caller authentication based on STIR and SHAKEN standards is the best approach to identify unlawful spoofing, and we will continue to invest and promote industry adoption of these standards. In the long run, the information from verifying calls in this

[24] Current STIR/SHAKEN standards only apply to end-to-end IP networks, so cannot be deployed on TDM networks.

environment can be used with analytical approaches to further enrich the information signaled to subscribers, as well as enhance a trace back process to more efficiently identify the source(s) of suspect calls.

Neustar, however, is concerned about the rate of adoption of the STIR and SHAKEN standards and the time it will take for any critical mass deployment of caller authentication utilizing these standards. Neustar supports further action by the Commission to establish industry timelines for adoption of mitigation techniques and associated metrics to gauge progress and effectiveness.

Even in a more ubiquitous state of caller authentication, Neustar proposes that information collected as part of verifying calls, including whether an originating call is digitally signed, should be only one source of data used to convey the most relevant and useful information about a call to a subscriber. Neustar does not favor the use of verification information alone to make provider-initiated blocking decisions but instead seeks to incorporate this information into meaningful context for subscribers (through their landline and/or mobile devices) so they can make informed decisions. Such an approach removes the risk of potentially blocking legitimate calls (and increased customer complaints) and eliminates imposing unnecessary costs (ultimately borne by customers) resulting from implementing and administering various data feeds into call processing procedures.

Neustar believes in most cases that subscribers are in the best position to determine if a call should be answered. Consequently, we suggest that the provider and vendor industry accelerate efforts to empower subscribers (and their devices/device applications) with the richest set of information to make the most informed decisions. Useful information, regarding incoming calls, including scoring for example, as determined by various centralized data analytics and reputation tools, can be delivered to any device today that supports conventional 15-character CNAM service, and begin to empower the mass consumer market.

The output of such data analytics tools can be delivered/signaled to subscribers in various ways using simple policy rules to modify the signaled CNAM based, for example, on a reputation score or score range that would result in a call signaled via a subscriber's caller ID display as "Suspect Number." As a further example, similar policy rules can be defined to modify the signaled CNAM based on the verification status as well. For example, a non-verified Caller ID could be signaled as "Unverified." For smartphones operating systems/applications, the signaled CNAM can be interpreted and expanded into a much richer, intuitive display for the subscriber.

Neustar has created a Trust Lab to test and integrate with providers and major mobile application providers being used or considered by wireless providers to battle robocalling and transform the calling experience for consumers. As a leading information services company, Neustar is commercializing a data analytics solution through collaboration with service providers. A key benefit of such solutions is that they are typically technology agnostic. More specifically, where caller authentication based on current STIR and SHAKEN standards require VoIP and SIP signaling, data analytics tools can support both traditional TDM/SS7 and VoIP/SIP networks.

Conventional 15-character CNAM service is likely to also be the only way for signaling the status of caller authentication to an anticipated broad set of devices that will be incapable of processing new in-band signaling of verification status, especially during the initial stages of implementation. Accurate CNAM, along with verified Caller ID, form a foundation for building a much better consumer phone experience.

With the explosion of smartphones, the consumer experience can be significantly enhanced with embedded applications that leverage the advances in mobile data (for incorporating out-of-band information on suspect calls), on-board processing and screen size/resolution. Such an approach channels effort into automated approaches that leverage existing infrastructure, allows subscribers to make more informed decisions, and eliminates the risk, especially in the immediate and near term, that providers will block legitimate calls.

While the subscriber is being empowered to make informed decisions about whether to answer a call, verification information can be incorporated into a more automated trace back process by providers and other third parties to more efficiently isolate the source(s) of suspect calls through the SHAKEN standard. The adoption of the currently defined caller authentication standards will, however, pose some challenges for providers still using TDM/SS7. STIR and SHAKEN currently assume a VoIP infrastructure and SIP signaling. Thus, for the foreseeable future, there are more magnified economic implications for adoption by various providers mostly entrenched in traditional TDM/SS7 network and signaling infrastructures.

H. While Protecting Legitimate Callers is a Laudable Goal, Establishing Such Protections Would be Challenging.

The FCC seeks comment on establishing a mechanism, such as a white list, to enable legitimate callers to avoid having their calls blocked by providers.[25] Aside from the NANPA and PA lists discussed above for invalid and unallocated telephone numbers, creating and managing whitelists (or blacklists) for purposes of provider-initiated blocking decisions is risky and problematic. These problems include: the criteria for getting on or off a list; the means for distributing and sharing such lists with service providers; and the consumer harm associated with

[25] *Robocalling Notice* ¶¶ 37-38.

delay in getting off the list or inadvertent disclosure of the list. Further, the ongoing management of such lists is likely to become unwieldy and add administrative costs.

Neustar believes that SHAKEN and STIR standards for authenticating Caller ID are an essential ingredient to combatting illegitimate spoofed calls, but making specific requirements around signing calls and using those as provider-initiated blocking criteria will be difficult given the pace at which such standards are likely to be implemented. Even in a more ubiquitous state of caller authentication, Neustar proposes that information collected as part of verifying calls, including whether an originating call is digitally signed or not, should still just be one source of data used to convey the most relevant and useful information about a call to a subscriber. The subscriber should be empowered to decide which calls to accept, which to ignore, and which to block.

The FCC also seeks comment on implementing a process to allow legitimate callers to notify providers when their calls are blocked and to require providers immediately to cease blocking calls when they learn that the calls are legitimate.[26] Consistent with Neustar's response above, such a process is not likely needed if decisions on answering calls are primarily left to subscribers or blocked locally on their device based on useful information.

IV. CONCLUSION

Neustar supports provider-initiated call blocking where it can be objectively determined that the apparent originating number is has been requested by its subscriber not to originated calls, or invalid or unallocated. Neustar can also support provider-initiated call blocking for unassigned numbers, but has concerns about how this can be implemented.

[26] *Robocalling Notice* ¶¶ 39-40.

In other cases, however, where there is subjective question about the legitimacy of a call, the risk of inadvertently shutting down legitimate traffic is too great. Neustar firmly believes that providers should use data analytics, crowd-sourcing, and caller authentication to provide more detailed information to the consumer via currently available Caller ID and CNAM displays. Where new IP and smartphone displays allow for more than a telephone number and 15 character name, the FCC should strongly encourage providers to display more detailed information. Consumers should be able to not only trust their Caller ID display, but also use the display to receive as much information as possible about the calling party in order to make the most informed decision about answering the call. The final solution to the problems of illegal spoofing and robocalling is not a single solution at all, but a mix of evolving solutions that involve both authorizing providers to block certain calls and empowering consumers to make more informed answering decisions on all other calls.

July 3, 2017

Respectfully submitted,

By: */s/ Leonard J. Kennedy*
____
Leonard J. Kennedy
Aaron N. Goldberger
Richard L. Fruchterman, III
NEUSTAR, INC.
1775 Pennsylvania Avenue N.W.
4th Floor
Washington, D.C. 20006